WHAT IS CLAIMED IS:

1. A method for regulating network access, the method comprising:

receiving a request for network access for a user identity;

identifying a type of connection that the user identity seeks to leverage if granted the network access requested;

identifying the user identity for which the request is submitted;

identifying one or more other user identities that are associated with the user identity;

determining whether the other user identities that are identified as being associated with the user identity have network access contemporaneously with the received request;

determining types of connections used to obtain the network access by the other user identities that are identified as being associated with the user identity and determined to have network access; and

determining whether to grant the user identity the network access requested based on the type of connections used by the other user identities that are identified as being associated with the user identity and determined to have network access.

2. The method of claim 1 wherein the user identity is a screen name or an Internet Protocol address and the network access is Internet access.

3. The method of claim 1 wherein the user identity is an e-mail address or a media access control address.

4. The method of claim 1 wherein the type of connection used by the user identity includes one of wireless, dial-up, digital subscriber line, and cable modem.

5. The method of claim 1 wherein the type of connections used by the other user identities includes one of wireless, dial-up, digital subscriber line, and cable modem

6. The method of claim 1 wherein the user identity includes an Internet Protocol address and identifying a type of connection includes identifying the type of connection based on the Internet Protocol address.

7. The method of claim 1 wherein the user identity includes a network identity and identifying a type of connection includes identifying the type of connection based on the network identity.

8. The method of claim 1 wherein the other user identities associated with the user identity are other user identities that are associated with the same online service account as the user identity.

9. The method of claim 1 wherein determining whether to grant access comprises applying a set of login rules to determine whether to grant access.

10. The method of claim 9, wherein applying the login rules results in denying access if a maximum number of concurrent logins has been reached.

11. The method of claim 10, wherein the concurrent logins comprise concurrent logins using the same type of connection as the type of connection used by the user identity to attempt to access the online service provider system.

12. The method of claim 9, wherein the login rules limit the number of concurrent logins to a maximum number of concurrent logins for a predetermined amount of time.

13. The method of claim 9, wherein the login rules vary based on user identity.

14. The method of claim 9, wherein the login rules limit the number of concurrent logins based on temporal constraints.

15. The method of claim 14, wherein the login rules limit the number of concurrent logins for one or more predetermined time intervals.

16. The method of claim 9, wherein the login rules limit the number of concurrent logins based on the existence of one or more identified conditions.

17. The method of claim 1, wherein determining whether to grant the user identity access comprises denying access and further comprises sending an access denied message to be perceived by a user associated with the user identity.

18. The method of claim 17, wherein the access denied message is configured to be perceived by the user as a graphical display.

19. The method of claim 17, wherein the access denied message includes information related to the reason why the access was denied.

20. The method of claim 17, wherein the access denied message includes data related to the other user identities.

21. The method of claim 20, wherein the access denied message includes data related to the types of connections used by the other user identities.

22. The method of claim 17, wherein the access denied message includes options configured to be selectable by the user.

23. The method of claim 22, further comprising receiving an option selection from the user and granting limited network access to the user identity associated with the user in response to the received option selection.

24. The method of claim 23, wherein the limited network access comprises network access for a limited duration of time.

25. The method of claim 23, wherein the limited network access comprises network access that is limited to exchanging communications with the other user identities.

26. The method of claim 22, further comprising receiving an option selection from the user and denying network access to one of the other user identities associated with the user identity in response to the received option selection.

27. The method of claim 26, wherein the other user identity that is denied access had access to the network contemporaneously with the received option selection.

28. The method of claim 27, further comprising granting network access to the user identity after denying network access to the other user identity.

29. The method of claim 22, further comprising receiving an option selection from the user and enabling the user to register for a network access service upgrade in response to the received option selection.

30. A computer system for regulating access to an online service provider system, the computer system comprising;

a customer account data store;

a system state data store; and

an authentication server configured to

receive a request for network access for a user identity,

identify a type of connection that the user identity seeks to leverage if granted the network access requested,

access the customer account data store to identify one or more other user identities associated with the user identity,

access the system state data store to determine whether the other user identities have network access contemporaneously with the received request and to determine the types of connections used to obtain the network access by the other user identities; and

determine whether to grant the user identity the network access requested based on the types of connections used by the other user identities that are identified as being associated with the user identity and determined to have network access.

31. The computer system of claim 30, wherein the customer account data store and the system state data store are a single integrated data store.

32. The computer system of claim 30 wherein the user identity is a screen name or an Internet Protocol address and the network access is Internet access.

33. The computer system of claim 30 wherein the user identity is an e-mail address or a media access control address.

34. The computer system of claim 30 wherein the type of connection used by the user identity includes one of wireless, dial-up, digital subscriber line, and cable modem.

35. The computer system of claim 30 wherein the type of connections used by the other user identities includes one of wireless, dial-up, digital subscriber line, and cable modem

36. The computer system of claim 30 wherein the authentication server is configured to determine whether to grant the user identity access by applying a set of login rules.

37. The computer system of claim 36, wherein applying the login rules results in denying access if a maximum number of concurrent logins has been reached.

38. The computer system of claim 37, wherein the concurrent logins comprise concurrent logins using the same type of connection as the type of connection used by the user identity to attempt to access the online service provider system.

39. The computer system of claim 36, wherein the login rules limit the number of concurrent logins to a maximum number of concurrent logins for a predetermined amount of time.

40. The computer system of claim 36, wherein the login rules vary based on user identity.

41. The computer system of claim 36, wherein the login rules limit the number of concurrent logins based on temporal constraints.

42. The computer system of claim 41, wherein the login rules limit the number of concurrent logins for one or more predetermined time intervals.

43. The computer system of claim 36, wherein the login rules limit the number of concurrent logins based on the existence of one or more identified conditions.

44. The computer system of claim 30, wherein the authentication server is further configured to deny access and send an access denied message to be perceived by a user associated with the user identity.

45. The computer system of claim 44, wherein the access denied message is configured to be perceived by the user as a graphical display.

46. The computer system of claim 44, wherein the access denied message includes information related to the reason why the access was denied.

47. The computer system of claim 44, wherein the access denied message includes data related to the other user identities.

48. The computer system of claim 47, wherein the access denied message includes data related to the types of connections used by the other user identities.

49. The computer system of claim 45, wherein the access denied message includes options configured to be selectable by the user.

50. The computer system of claim 49, wherein the authentication server is further configured to receive an option selection from the user and grant limited network access to the user identity associated with the user in response to the received option selection.

51. The computer system of claim 50, wherein the limited network access comprises network access for a limited duration of time.

52. The computer system of claim 50, wherein the limited network access comprises network access that is limited to exchanging communications with the other user identities.

53. The computer system of claim 49, wherein the authentication server is further configured to receive an option selection from the user and deny network access to one of the other user identities associated with the user identity in response to the received option selection.

54. The computer system of claim 53, wherein the other user identity that is denied access had access to the network contemporaneously with the received option selection.

55. The computer system of claim 54, wherein the authentication server is further configured to grant network access to the user identity after denying network access to the other user identity.

56. The computer system of claim 49, wherein the authentication server is further configured to receive an option selection from the user and enable the user to register for a network access service upgrade in response to the received option selection.

57. An apparatus for regulating network access, the apparatus comprising:

means for receiving a request for network access for a user identity;

means for identifying a type of connection that the user identity seeks to leverage if granted the network access requested;

means for identifying the user identity for which the request is submitted;

means for identifying one or more other user identities that are associated with the user identity;

means for determining whether the other user identities that are identified as being associated with the user identity have network access contemporaneously with the received request;

means for determining types of connections used to obtain the network access by the other user identities that are identified as being associated with the user identity and determined to have network access; and

means for determining whether to grant the user identity the network access requested based on the type of connections used by the other user identities that are identified as being associated with the user identity and determined to have network access.